CONFIDENTIEL JUSQU'A LA REUNION AVEC LA COMMISSION DU SUIVI

COMITÉ PERMANENT DE CONTRÔLE
DES SERVICES DE RENSEIGNEMENT ET DE SÉCURITÉ

RAPPORT D'ACTIVITÉS 2020
LE CONTRÔLE DES MÉTHODES PARTICULIÈRES ET DE CERTAINES MÉTHODES ORDINAIRES DE RENSEIGNEMENT

LE CONTRÔLE DES MÉTHODES PARTICULIÈRES ET DE CERTAINES MÉTHODES ORDINAIRES DE RENSEIGNEMENT

L'année 2020 a marqué le dixième anniversaire de la Loi du 4 février 2010 relative aux méthodes de recueil des données par les services de renseignement et de sécurité (connu comme la Loi sur les méthodes particulières, en abrégé la Loi MRD[1]). Cet événement méritait d'être célébré. Aussi, le Comité a organisé, le 31 janvier 2020, sous les auspices de la Chambre des représentants, le colloque intitulé 'Bijzondere inlichtingenmethoden in de schijnwerpers – Les méthodes particulières de renseignement : de l'ombre à la lumière'.[2]

Avec l'entrée en vigueur de cette loi, que la Loi du 30 mars 2017[3] (la 'Loi d'actualisation MRD') a profondément modifiée, les possibilités de recueil d'informations par les deux services de renseignement ont été considérablement élargies.

Lorsque le législateur en 2010 a finalement décidé de doter les services de renseignement de nouvelles compétences, une mission importante a, par la même occasion, été confiée au Comité permanent R. Le Comité devait, conjointement à la Commission BIM, contrôler l'exécution de ces MRD, lesquelles sont par définition très intrusive pour les droits et libertés individuels. L'article 35 L. Contrôle impose une transparence au Comité dans les activités qu'il mène dans ce contexte.

Le présent chapitre reprend donc les chiffres détaillés de la mise en œuvre par la Sûreté de l'État (VSSE) et par le Service Général du Renseignement et de la Sécurité (SGRS) des méthodes spécifiques et exceptionnelles (regroupées en 'méthodes particulières de renseignement') et de certaines méthodes ordinaires, pour lesquelles le Comité s'est vu confier une mission de contrôle supplémentaire. De plus, il est fait rapport sur la manière dont le Comité assure sa mission de contrôle juridictionnelle sur ces méthodes. Outre une série de chiffres sur le nombre de décisions et la manière dont le Comité a été saisi, la substance des décisions finales du Comité permanent R est également reprise. La jurisprudence a été expurgée des données opérationnelles ; seuls sont mentionnés les éléments qui présentent un intérêt d'un point de vue juridique.

---

1 *M.B.* 10 mars 2010.

2 Y étaient représentés : le ministre de la Justice, différents Députés, membres des services de renseignement et de sécurité, universitaires, journalistes, membres d'institutions des droits de l'homme, du barreau et du monde judiciaire, des organes de contrôle ainsi que des contacts internationaux. Un compte-rendu, sous la forme d'un livre, a été publié à ce propos : J. VANDERBORGHT (ed.), *Bijzondere inlichtingenmethoden in de schijnwerpers - Les méthodes particulières de renseignement: de l'ombre à la lumière,* Intersentia, Antwerpen, 2020, 151 p.

3 *M.B.* 28 avril 2017.

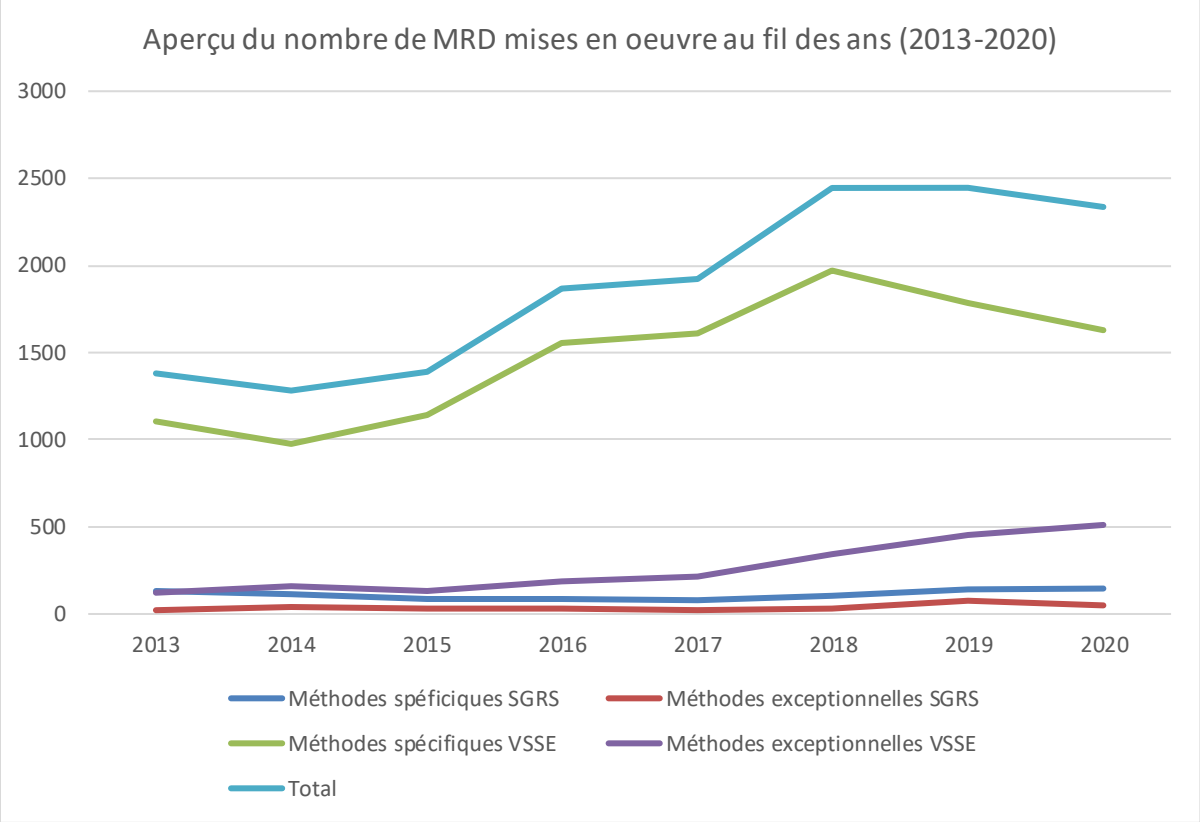
II.1. LES CHIFFRES RELATIFS AUX MÉTHODES PARTICULIÈRES ET À CERTAINES MÉTHODES ORDINAIRES

Entre le 1er janvier et le 31 décembre 2020, 2337 autorisations ont été émises par les deux services de renseignement confondus pour l'utilisation de méthodes particulières de renseignement : 2140 par la VSSE (1629 spécifiques et 511 exceptionnelles) et 197 par le SGRS (146 spécifiques et 51 exceptionnelles). Selon les responsables MRD de la VSSE et du SGRS, la pandémie de COVID n'a eu aucun impact sur le nombre de méthodes particulières de renseignement mises en oeuvre.

Le tableau ci-dessous établit une comparaison avec les chiffres des années précédentes.

	SGRS		VSSE		TOTAL
	Méthodes spécifiques	**Méthodes exceptionnelles**	**Méthodes spécifiques**	**Méthodes exceptionnelles**	
2013	131	23	1102	122	1378
2014	114	36	976	156	1282
2015	87	34	1143	128	1392
2016	88	33	1558	189	1868
2017	79	22	1612	210	1923
2018	102	28	1971	344	2445
2019	138	76	1781	449	2444
2020	146	51	1629	511	2337

Cela donne schématiquement :



Après une augmentation constante du nombre de MRD mises en œuvre ces dernières années et une stagnation en 2019, on remarque pour la première fois une diminution (négligeable) : le nombre total de méthodes utilisées est resté plutôt stable en 2020. Il convient néanmoins de noter que plusieurs targets (tels que des personnes, des organisations, des lieux, des objets, des moyens de communication, etc.) peuvent être visés dans une même autorisation.

La VSSE se taille la part du lion, avec 91,5 % des méthodes mises en œuvre.

Une ventilation de ces chiffres permet de constater que l'augmentation du nombre de méthodes spécifiques par le SGRS se poursuit, passant de 138 à 146. Le nombre de méthodes exceptionnelles mises en œuvre connaît toutefois une forte diminution d'environ un tiers, passant de 76 à 51.[4]

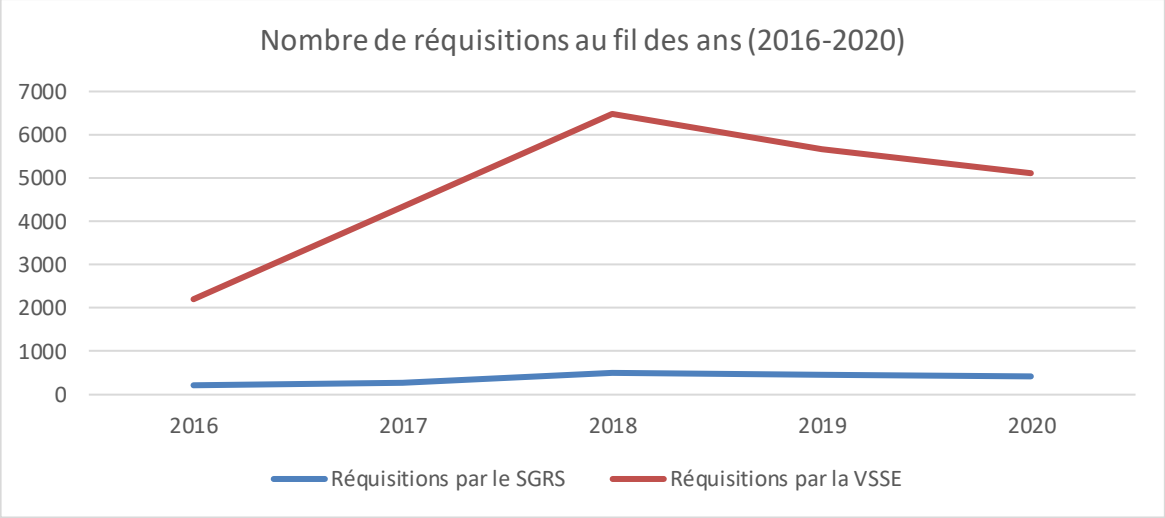
À la VSSE, on observe la tendance inverse, c'est-à-dire une diminution remarquable de l'utilisation des méthodes spécifiques (de 1781 en 2019 à 1629 en 2020) et une nouvelle hausse sensible de l'utilisation des méthodes exceptionnelles (de 449 en 2019 à 511 en 2020, soit une hausse d'environ 14 %). Le Comité se limite ici à reprendre les chiffres bruts.

[4] Ce qui est important dans ce contexte, c'est que le SGRS dispose également de compétences particulières pour le recueil d'informations, telles que réglées dans les articles 44 et suiv. L.R&S. Voir à ce propos 'Chapitre III. Le contrôle des interceptions à l'étranger, des prises d'images et des intrusions dans des systèmes informatiques'.

En ce qui concerne les méthodes ordinaires qui consistent à adresser une réquisition à des opérateurs et fournisseurs (*providers*) de télécom afin d'identifier certains moyens de communication (cf. art. 16/2 L.R&S), on note de nouveau une diminution (environ 10 %). On dénombre une dizaine de réquisitions de moins au SGRS par rapport à 2019, contre plus de 550 réquisitions de moins du côté de la VSSE).

	Réquisitions par le SGRS	**Réquisitions par la VSSE**
2016	216	2203
2017	257	4327
2018	502	6482
2019	442	5674
2020	433	5123

Cela donne schématiquement :



Le Comité avait déjà indiqué[5] qu'« *[il] ne [pouvait] nier qu'un nombre beaucoup plus élevé d'identifications ont été effectuées depuis l'introduction de la procédure assouplie visée à l'article 16/2 L.R&S ».* Le nombre de réquisitions en 2020, bien que toujours en baisse, demeure assez important. Dans l'exercice de sa compétence de contrôle générale, le Comité en a examiné les motifs ; les résultats ont été repris dans l'enquête de contrôle ouverte en 2019 et intitulée *'enquête de contrôle sur l'application et le contrôle interne des services de renseignement des méthodes et instruments récemment insérés ou adaptés par le législateur et dont un rôle de contrôle spécifique a été attribué au Comité permanent R'* (cf. I.11.1).

[5] COMITÉ PERMANENT R, *Rapport d'activités 2017*, 43.

II.1.1. MÉTHODES UTILISÉES PAR LE SGRS

II.1.1.1. Méthodes ordinaires 'plus'

Identification de l'utilisateur de télécommunications

L'identification de l'utilisateur de télécommunications (par ex. d'un numéro de GSM ou d'une adresse IP) ou d'un moyen de communication utilisé est considérée comme une méthode ordinaire, dans la mesure où elle a lieu via une réquisition auprès les opérateurs et fournisseurs (*providers*) de télécom ou via un accès direct aux fichiers des clients.[6] La réglementation prévoit une obligation pour les services de renseignement de tenir un registre de toutes les identifications requises et de toutes les identifications obtenues par accès direct.[7] Conformément à cette même réglementation, le Comité doit recevoir, sur une base mensuelle, une liste des identifications requises et de chaque accès. Le SGRS a, quant à lui, enregistré une légère diminution du nombre de réquisitions, passant de 442 en 2019 à 433 en 2020. Cette thématique a également fait l'objet d'une enquête de contrôle ouverte en 2019 (*supra*).

Identification du détenteur d'une carte prépayée

L'article 16/2 L.R&S mentionne ce qui suit : '*§ 2. Les services de renseignement et de sécurité peuvent, dans l'intérêt de l'exercice de leurs missions, requérir le concours d'une banque ou d'une institution financière pour procéder à l'identification de l'utilisateur final d'une carte prépayée visée dans l'article 127 de la loi du 13 juin 2005 relative aux communications électroniques, sur la base de la référence d'une transaction bancaire électronique qui est liée à la carte prépayée et qui a préalablement été communiquée par un opérateur ou un fournisseur en application du paragraphe 1er.*' Comme en 2018 et en 2019, les deux services de renseignement n'ont pas encore employé cette méthode.

Accès aux données PNR

Début 2017,[8] une loi a introduit la possibilité pour les services de renseignement d'avoir accès aux informations détenues par l'Unité d'information des passagers, et ce par le biais de

---

6 Lorsque l'identification a lieu à l'aide d'un moyen technique (et donc pas via une réquisition à un opérateur), la collecte reste une méthode spécifique (art. 18/7 § 1er L.R&S).

7 La possibilité pour les services de renseignement de demander de telles données d'identification via un accès direct à des fichiers clients des opérateurs et fournisseurs de télécommunications, créée à l'article 16/2, § 1er, dernier alinéa L.R&S, est restée sans effet à ce jour.

8 Loi du 25 décembre 2016 (*M.B.* 25 janvier 2017).

recherches ciblées (art. 16/3 L.R&S et art. 27 Loi PNR du 25 décembre 2016). Le Comité est informé de l'utilisation de cette méthode et peut l'interdire le cas échéant.[9]

La réglementation PNR permet également de réaliser ce que l'on appelle une 'évaluation préalable', qui consiste à vérifier automatiquement la correspondance entre les données PNR et les listes ou fichiers de noms des services de renseignement et à envoyer des informations sur la base de *hits* validés (art. 24 Loi PNR). Le nombre de recherches effectuées dans les données PNR a diminué, passant de 38 en 2019 à 28 en 2020.

Utilisation d'images enregistrées par les caméras des services de police

La Loi du 30 novembre 1998 organique des services de renseignement et de sécurité a été adaptée par la Loi du 21 mars 2018 (*M.B.* 16 avril 2018) pour permettre aux services de renseignement d'utiliser des images enregistrées par les caméras des services de police. Une nouvelle méthode ordinaire a été introduite à cet effet (art. 16/4 §2 L.R&S).[10] [11]

Les chiffres

Méthodes ordinaires (SGRS)	Nombre d'autorisations
Identification de l'utilisateur de télécommunications	433
Identification du détenteur d'une carte prépayée	0
Recherches ciblées de données PNR	28
Transmission de données PNR sur la base de *hits*	Non communiqué
Utilisation d'images enregistrées par les caméras des services de police	Pas en vigueur[12]

II.1.1.2. Les méthodes spécifiques

Le tableau ci-dessous reprend les chiffres relatifs à l'application des méthodes spécifiques par le SGRS. On en distingue sept.

---

9 Contrairement à ce qui s'applique aux méthodes reprises à l'article 16/2 L.R&S, il n'était pas prévu qu'un rapport doive être rédigé à l'intention du Parlement. L'article 35 § 2 L. Contrôle n'a, en effet, pas été adapté. Suivant la suggestion émise par la Commission de suivi, le Comité a décidé de reprendre ces chiffres dans son rapport annuel et de ne pas attendre une éventuelle modification de la loi.

10 Cette même loi a étendu la possibilité d'observation spécifique et exceptionnelle existante (articles 18/4 § 3 et 18/11 § 3 L.R&S).

11 Début 2019, le Conseil des ministres a approuvé un projet d'arrêté royal en application de l'art. 16 § 4 L.R&S, qui a été soumis à l'avis du Comité permanent R. Cet avis 002/CPR-ACC/2019 du 9 avril 2019 peut être consulté sur le site internet du Comité (www.comiteri.be).

12 Le champ d'application de l'article 16/4 L.R&S (par exemple en ce qui concerne les consultations de la Direction de l'information policière et des moyens ICT (DRI) de la Police fédérale) fait l'objet d'une analyse juridique (2021).

Méthodes spécifiques (SGRS)	Nombre d'autorisations
Observer, à l'aide d'un moyen technique, dans des lieux accessibles au public ou observer, à l'aide ou non d'un moyen technique, dans un lieu non accessible au public qui n'est pas soustrait à la vue (art. 18/4 L.R&S)[13]	6
Inspecter des lieux accessibles au public, à l'aide d'un moyen technique, inspecter le contenu d'objets verrouillés ou les emporter (art. 18/5 L.R&S)	0
Prendre connaissance de données d'identification d'un trafic postal et requérir le concours d'un opérateur postal (art.18/6 L.R&S)	0
Requérir des données de transport et de voyage auprès de fournisseurs privés de service en matière de transport ou de voyage (art. 18/6/1 L.R&S)	2
Identifier, à l'aide d'un moyen technique, les services et de moyens de communications électroniques auxquels une personne déterminée est abonnée ou qui sont habituellement utilisés par une personne déterminée (art. 18/7 §1, 1° L.R&S)	2
Requérir le concours de l'opérateur d'un réseau de communications électroniques afin d'obtenir les données relatives à la méthode de paiement, identifier le moyen de paiement et le moment du paiement de l'abonnement ou de l'utilisation du service de communications électroniques (art. 18/7 §1, 2° L.R&S)	0
Prendre connaissance des données d'appel d'un trafic de communications électroniques et requérir le concours d'un opérateur (art. 18/8 §1, 1°L.R&S)	69
Prendre connaissance des données de localisation d'un trafic de communications électroniques et requérir le concours d'un opérateur (art. 18/8 §1, 2° L.R&S)	67
TOTAL	**146**

En ce qui concerne la mise en œuvre des méthodes spécifiques, ce sont le repérage des données d'appel d'un trafic de communications électroniques' (art. 18/8 L.R&S) et la 'prise de connaissance de données de localisation' (art. 18/8 L.R&S), tous deux assortis d'une réquisition du concours d'un opérateur, qui se hissent clairement en tête du classement (136 des 146 méthodes spécifiques mises en œuvre). L'observation dans des lieux accessibles au public à l'aide d'un moyen technique a diminué de moitié, passant de 12 en 2019 à 6 en 2020.

II.1.1.3. Les méthodes exceptionnelles

Dans le cadre de ses missions visées aux articles 11, § 1er, 1° à 3° en 5°, et § 2 L.R&S, le SGRS peut mettre en œuvre différentes méthodes exceptionnelles :

[13] La Loi du 21 mars 2018 (*M.B.* 16 avril 2018) a ajouté un nouveau paragraphe à l'article 18/4 L.R&S pour permettre aux services de renseignement d'utiliser des images enregistrées par les caméras des services, et ce afin d'effectuer des observations en temps réel. Cette méthode, qui nécessite un accès direct aux informations visées n'a pas encore été opérationnalisée.

Méthodes exceptionnelles (SGRS)	Nombre d'autorisations
Observer, à l'aide ou non de moyens techniques, des lieux non accessibles au public qui sont soustraits à la vue et pénétrer dans des lieux non accessibles au public qui sont soustraits ou non à la vue pour exécuter une observation, installer un moyen technique, ouvrir un objet ou l'emporter (art. 18/11 L.R&S)[14]	2
Inspecter, à l'aide ou non de moyens techniques, des lieux non accessibles au public, ainsi que l'inspection du contenu d'objets verrouillés ou non qui s'y trouvent (art. 18/12 L.R&S)	0
Recourir à une personne morale visée à l'article 13/3, § 1er L.R&S afin de collecter des données	0
Ouvrir et prendre connaissance du courrier confié ou non à un opérateur postal (art. 18/14 L.R&S)	0
Collecter des données concernant des comptes bancaires et des transactions bancaires (art. 18/15 L.R&S)	6
S'introduire dans un système informatique (article 18/16 L.R&S)	4
Écouter, prendre connaissance et enregistrer des communications (art. 18/17 L.R&S)	39
TOTAL	**51**

La forte diminution en pourcentage (plus de 30 %) du nombre de méthodes exceptionnelles mises en œuvre par le SGRS se situe principalement au niveau de la 'collecte de données concernant les comptes bancaires et les transactions bancaires' (art. 18/15 L.R&S) : si cette méthode avait encore été employée à 20 reprises en 2019, elle ne l'a été qu'à 6 reprises en 2020. La même tendance à la baisse s'observe pour les intrusions dans un système informatique (18/16 L.R&S) ; il y en a eu deux fois moins par rapport à 2019 (de 8 à 4).

II.1.1.4. Les missions et les menaces justifiant le recours aux méthodes ordinaires et particulières [15]

Le SGRS est autorisé à employer les méthodes spécifiques et exceptionnelles dans le cadre de quatre missions et tenant compte de différentes natures de menaces.

1. **La mission de renseignement (art. 11, 1° L.R&S)**
   Le recueil, l'analyse et le traitement du renseignement relatif aux facteurs qui influencent ou peuvent influencer la sécurité nationale et internationale dans la mesure où les Forces armées sont ou pourraient être impliquées, en fournissant un soutien en renseignement à leurs opérations en cours ou à leurs éventuelles opérations à venir. Le recueil, l'analyse et le traitement du renseignement relatif à toute activité qui menace ou pourrait menacer les intérêts suivants :

---

14 La Loi du 21 mars 2018 (*M.B.* 16 avril 2018) a ajouté un nouveau paragraphe à l'article 18/4 L.R&S pour permettre aux services de renseignement d'utiliser des images enregistrées par les caméras des services, et ce afin d'effectuer des observations en temps réel. Cette méthode, qui nécessite un accès direct aux informations visées n'a pas encore été opérationnalisée.

15 Plusieurs intérêts et menaces peuvent figurer dans une même autorisation.

- l'intégrité du territoire national ou la survie de tout ou partie de la population ;
- les plans de défense militaires ;
- le potentiel économique et scientifique en rapport avec la défense ;
- l'accomplissement des missions des Forces armées ;
- la sécurité des ressortissants belges à l'étranger.

2. **Veiller au maintien de la sécurité militaire (art. 11, 2° L.R&S)**
   - la sécurité militaire du personnel relevant du ministre de la Défense nationale ;
   - les installations militaires, armes, munitions, équipements, plans, écrits, documents, systèmes informatiques et de communications ou autres objets militaires ;
   - dans le cadre des cyberattaques de systèmes informatiques et de communications militaires ou de ceux que le ministre de la Défense nationale gère, neutraliser l'attaque et en identifier les auteurs, sans préjudice du droit de réagir immédiatement par une propre cyberattaque, dans le respect des dispositions du droit des conflits armés.
3. **La protection de secrets (art. 11, 3° L.R&S)**
   La protection du secret qui, en vertu des engagements internationaux de la Belgique ou afin d'assurer l'intégrité du territoire national et l'accomplissement des missions des Forces armées, s'attache aux installations militaires, armes, munitions, équipements, aux plans, écrits, documents ou autres objets militaires, aux renseignements et communications militaires, ainsi qu'aux systèmes informatiques et de communications militaires ou ceux que gère le ministre de la Défense nationale.
4. **La recherche, l'analyse et le traitement du renseignement relatif aux activités des services de renseignement étrangers sur le territoire belge (art. 11, 5°, L.R&S).**

Ces méthodes ne peuvent donc pas être utilisées dans le cadre d'enquêtes de sécurité ou d'autres missions assignées au SGRS par ou conformément à des lois particulières (par ex. effectuer des vérifications de sécurité pour des candidats militaires). Toutefois, depuis l'entrée en vigueur de la Loi du 30 mars 2017, la mise en œuvre de méthodes particulières n'est plus limitée au territoire belge (art. 18/1, 2° L.R&S). La pratique a montré que plusieurs menaces peuvent figurer dans une même autorisation.

Environ deux tiers des méthodes spécifiques et exceptionnelles sont utilisés par le SGRS dans le cadre de la mission de recherche, d'analyse et de traitement du renseignement relatif aux activités des services de renseignements étrangers sur le territoire belge (art. 11, 5° L.R&S).[16] On ne peut cependant pas en déduire que, depuis 2017, le SGRS suit un 'nouveau genre' de menace. En effet, le suivi de services étrangers était auparavant plus vite associé à la mission de renseignement dans le contexte de la lutte contre l'espionnage. On peut encore noter que le nombre de MRD mises en œuvre dans le cadre des menaces 'terrorisme' et 'extrémisme' ont connu une hausse sensible, au détriment de la menace 'ingérence', qui a diminué de moitié.

[16] Aucune méthode particulière de renseignement n'a été utilisée à l'étranger par l'SGRS en 2020.

NATURE DE LA MENACE	NOMBRE EN 2020
Espionnage	139
Ingérence	19
Extrémisme	20
Terrorisme	19
Organisations criminelles	-
Autre	-
Total	197

Contrairement à la mise en œuvre de méthodes particulières, le Comité ne dispose pas de données chiffrées relatives à la menace visée et aux intérêts à défendre en ce qui concerne les méthodes ordinaires dont il est question dans le présent chapitre. Dans son précédent rapport d'activités, le Comité recommandait aux services de consigner ces données et de les tenir à disposition.[17] Étant donné que ce n'est pas encore le cas, le Comité réitère sa recommandation.

II.1.2. LES MÉTHODES UTILISÉES PAR LA VSSE

II.1.2.1. Les méthodes ordinaires 'plus'

Méthodes ordinaires (VSSE)	Nombre d'autorisations
Identification de l'utilisateur de télécommunications	5123
Identification du détenteur d'une carte prépayée	0
Recherches ciblées de données PNR	30
Transmission de données PNR sur la base de *hits*	Non communiqué
Utilisation d'images enregistrées par les caméras des services de police	Pas en vigueur[18]

Pour rappel, le Comité va procéder à un examen approfondi de la manière dont cette méthode est mise en œuvre dans son enquête de contrôle initiée en 2019.

17 COMITÉ PERMANENT R, *Rapport d'activités 2017*, 43.

18 Le champ d'application de l'article 16/4 L.R&S (par exemple en ce qui concerne les consultations de la Direction de l'information policière et des moyens ICT (DRI) de la Police fédérale) fait l'objet d'une analyse juridique (2021).

II.1.2.2. Les méthodes spécifiques

Méthodes spécifiques (VSSE)	Nombre d'autorisations
Observer, à l'aide d'un moyen technique, dans des lieux accessibles au public ou observer, à l'aide ou non d'un moyen technique, dans un lieu non accessible au public qui n'est pas soustrait à la vue (art. 18/4 L.R&S)	245
Inspecter des lieux accessibles au public, à l'aide d'un moyen technique, inspecter le contenu d'objets verrouillés ou les emporter (art. 18/5 L.R&S)	0
Prendre connaissance de données d'identification d'un trafic postal et requérir le concours d'un opérateur postal (art.18/6 L.R&S)	1
Requérir des données de transport et de voyage auprès de fournisseurs privés de service en matière de transport ou de voyage (art. 18/6/1 L.R&S)	70
Identifier, à l'aide d'un moyen technique, les services et de moyens de communications électroniques auxquels une personne déterminée est abonnée ou qui sont habituellement utilisés par une personne déterminée (art. 18/7 §1, 1° L.R&S)	46
Requérir le concours de l'opérateur d'un réseau de communications électroniques afin d'obtenir les données relatives à la méthode de paiement, identifier le moyen de paiement et le moment du paiement de l'abonnement ou de l'utilisation du service de communications électroniques (art. 18/7 §1, 2° L.R&S)	0
Prendre connaissance des données d'appel d'un trafic de communications électroniques et requérir le concours d'un opérateur (art. 18/8 L.R&S)	650
Prendre connaissance des données de localisation d'un trafic de communications électroniques et requérir le concours d'un opérateur (art. 18/8 L.R&S)	617
TOTAL	**1629**

Comme susmentionné, le nombre de méthodes spécifiques mises en œuvre en 2020 par rapport à 2019 a clairement diminué, passant de 1781 à 1629 méthodes. On constate que cette diminution est graduelle pour pratiquement toutes les méthodes spécifiques, à l'exception de la réquisition des données de transport et de voyage auprès de fournisseurs privés de service en matière de transport ou de voyage, qui a considérablement augmenté, passant de 48 en 2019 à 70 en 2020.

II.1.2.3. Les méthodes exceptionnelles

Méthodes exceptionnelles (VSSE)	Nombre d'autorisations
Observer, à l'aide ou non de moyens techniques, des lieux non accessibles au public qui sont soustraits à la vue et pénétrer dans des lieux non accessibles au public qui sont soustraits ou non à la vue pour exécuter une observation, installer un moyen technique, ouvrir un objet ou l'emporter (art. 18/11 L.R&S)[19]	9
Inspecter, à l'aide ou non de moyens techniques, des lieux non accessibles au public, ainsi que l'inspection du contenu d'objets verrouillés ou non qui s'y trouvent (art. 18/12 L.R&S)	8
Recourir à une personne morale visée à l'article 13/3, § 1er L.R&S afin de collecter des données	0
Ouvrir et prendre connaissance du courrier confié ou non à un opérateur postal (art. 18/14 L.R&S)	11
Collecter des données concernant des comptes bancaires et des transactions bancaires (art. 18/15 L.R&S)	186
S'introduire dans un système informatique (article 18/16 L.R&S)	74
Écouter, prendre connaissance et enregistrer des communications (art. 18/17 L.R&S)	223
TOTAL	**511**

Contrairement à la mise en œuvre des méthodes spécifiques, le nombre de méthodes exceptionnelles mises en œuvre par la VSSE est en constante augmentation (+ 14 % par rapport à 2019). Cette hausse s'explique entièrement par l'utilisation de la méthode 'Collecte des données concernant des comptes bancaires et des transactions bancaires' (art. 18/15 L/R&S) qui a plus que doublé, passant de 95 en 2019 à 186 en 2020) et de la méthode 'Intrusion dans un système informatique' (art 18/16 L.R&S), qui est passé de 48 en 2019 à 74 en 2020). Toutes les autres méthodes exceptionnelles ont été moins utilisées qu'en 2019.

II.1.2.4. Les menaces et les intérêts justifiant le recours aux méthodes particulières

Le tableau suivant reprend les menaces (potentielles) dans le cadre desquelles la VSSE a accordé des autorisations spécifiques et exceptionnelles. Une méthode peut naturellement viser plusieurs menaces. La VSSE peut utiliser les méthodes spécifiques dans le cadre de toutes les menaces qui entrent dans ses compétences (art. 8 L.R&S). La loi définit les diverses notions comme suit :

1. L'espionnage : le recueil ou la livraison d'informations non accessibles au public, et le fait d'entretenir des intelligences de nature à les préparer ou à les faciliter ;

[19] La Loi du 21 mars 2018 (*M.B.* 16 avril 2018) a ajouté un nouveau paragraphe à l'article 18/4 L.R&S pour permettre aux services de renseignement d'utiliser des images enregistrées par les caméras des services, et ce afin d'effectuer des observations en temps réel. Cette méthode, qui nécessite un accès direct aux informations visées n'a pas encore été opérationnalisée.

2. Le terrorisme : le recours à la violence à l'encontre de personnes ou d'intérêts matériels, pour des motifs idéologiques ou politiques, dans le but d'atteindre ses objectifs par la terreur, l'intimidation ou les menaces ;
   Processus de radicalisation : un processus influençant un individu ou un groupe d'individus de telle sorte que cet individu ou ce groupe d'individus soit mentalement préparé ou disposé à commettre des actes terroristes ;
3. L'extrémisme : les conceptions ou les visées racistes, xénophobes, anarchistes, nationalistes, autoritaires ou totalitaires, qu'elles soient à caractère politique, idéologique, confessionnel ou philosophique, contraires, en théorie ou en pratique, aux principes de la démocratie ou des droits de l'homme, au bon fonctionnement des institutions démocratiques ou aux autres fondements de l'État de droit ;
4. La prolifération : le trafic ou les transactions relatives aux matériaux, produits, biens ou know-how pouvant contribuer à la production ou au développement de systèmes d'armement non conventionnels ou très avancés. Sont notamment visés dans ce cadre le développement de programmes d'armement nucléaire, chimique et biologique, les systèmes de transmission qui s'y rapportent, ainsi que les personnes, structures ou pays qui y sont impliqués ;
5. Les organisations sectaires nuisibles, c'est-à-dire tout groupement à vocation philosophique ou religieuse, ou se prétendant tel, qui, dans son organisation ou sa pratique, se livre à des activités illégales dommageables, nuit aux individus ou à la société ou porte atteinte à la dignité humaine ;
6. L'ingérence : la tentative d'influencer des processus décisionnels par des moyens illicites, trompeurs ou clandestins ;
7. Les organisations criminelles, c'est-à-dire toute association structurée de plus de deux personnes, établie dans le temps, en vue de commettre de façon concertée des crimes et délits, pour obtenir, directement ou indirectement, des avantages patrimoniaux, en utilisant l'intimidation, la menace, la violence, des manœuvres frauduleuses ou la corruption ou en recourant à des structures commerciales ou autres pour dissimuler ou faciliter la réalisation des infractions. Sont visées dans ce cadre les formes et structures des organisations criminelles qui se rapportent intrinsèquement aux activités visées dans des menaces précédentes ou qui peuvent avoir des conséquences déstabilisantes sur le plan politique ou socio-économique.

Depuis l'entrée en vigueur de la Loi du 30 mars 2017, les méthodes particulières de renseignement peuvent également être mises en œuvre *'à partir du territoire du Royaume'*, et donc plus uniquement *'sur'* le territoire (art. 18/1, 1° L.R&S).

En considérant que plusieurs menaces peuvent figurer dans une même autorisation, les chiffres sont les suivants :

NATURE DE LA MENACE	**NOMBRE EN 2020**
Espionnage	816
Ingérence	27
Extrémisme	296
Prolifération	3
Organisations sectaires nuisibles	0
Terrorisme	998
Organisations criminelles	0
Suivi des activités des services étrangers en Belgique	(inclus dans les chiffres ci-dessus)
TOTAL	**2140**

Les chiffres repris ci-dessus montrent que le 'terrorisme', pour ce qui est de la mise en œuvre de MRD en 2020, a certes diminué (de 1118 à 998), mais que cette menace demeure la priorité absolue de la VSSE en 2020, suivie de près par la menace 'espionnage' (816). On peut constater à la VSSE, tout comme au SGRS, une forte diminution du nombre de 'dossiers d'ingérence' (de 87 en 2019 à 27 en 2020). Étant donné que les organisations sectaires nuisibles et les organisations criminelles ne font plus l'objet d'un suivi actif depuis 2015, il ne faut pas s'étonner que ces menaces ne figurent pas dans les chiffres.

La compétence de la VSSE n'est pas seulement définie par la nature de la menace. Le service n'est autorisé à intervenir que pour la sauvegarde d'intérêts bien déterminés :

1. La sûreté intérieure de l'État et la pérennité de l'ordre démocratique et constitutionnel, c'est-à-dire :
   a) la sécurité des institutions de l'État et la sauvegarde de la continuité du fonctionnement régulier de l'État de droit, des institutions démocratiques, des principes élémentaires propres à tout État de droit, ainsi que des droits de l'homme et des libertés fondamentales ;
   b) la sécurité et la sauvegarde physique et morale des personnes et la sécurité et la sauvegarde des biens.
2. La sûreté extérieure de l'État et les relations internationales : la sauvegarde de l'intégrité du territoire national, de la souveraineté et de l'indépendance de l'État, des intérêts des pays avec lesquels la Belgique poursuit des objectifs communs, ainsi que des relations internationales et autres que la Belgique entretient avec des États étrangers et des institutions internationales ou supranationales.
3. La sauvegarde des éléments essentiels du potentiel économique et scientifique.

Comme le SGRS, la VSSE combine plusieurs intérêts. On peut néanmoins mentionner que la 'sauvegarde des éléments essentiels du potentiel économique et scientifique' n'apparaissait pas dans les chiffres comme étant un intérêt.

Pour rappel, le Comité ne dispose pas des chiffres relatifs à la menace visée et aux intérêts à défendre en ce qui concerne les méthodes ordinaires dont il est question dans le présent chapitre.

II.2. LES ACTIVITÉS DU COMITÉ PERMANENT R EN SA QUALITÉ D'ORGANE (JURIDICTIONNEL) ET D'AUTEUR D'AVIS PRÉJUDICIELS

II.2.1. CONTRÔLE DE CERTAINES MÉTHODES ORDINAIRES

II.2.1.1. Généralités

Le contrôle de certaines méthodes ordinaires est réglementé de manière différente pour chacune d'entre elles.

En ce qui concerne l'identification de l'utilisateur de télécommunications (et l'identification de l'utilisateur d'une carte prépayée qui y est associée), la loi n'a pas instauré de contrôle spécifique. À l'article 16/2 § 4 L.R&S, il est seulement stipulé que la liste des identifications requises et de tous les accès directs doit être communiquée chaque mois au Comité. Comme déjà indiqué, le Comité reçoit uniquement le nombre de réquisitions. Il a toutefois proposé de contrôler annuellement une sélection de réquisitions.[20] Ce contrôle a débuté en 2020. Le Comité a décidé de reprendre cette thématique dans l'enquête qu'il a initiée en 2019 et qui est intitulée *'enquête de contrôle sur l'application et le contrôle interne des services de renseignement des méthodes et instruments récemment insérés ou adaptés par le législateur et dont un rôle de contrôle spécifique a été attribué au Comité permanent R.'*

En ce qui concerne l'accès aux données PNR, qui sont détenues par l'Unité d'information des passagers, l'article 16/3 L.R&S dispose que c'est le dirigeant du service qui doit décider de tout accès, et ce *'de façon dûment motivée'*. Le Comité doit en être informé *et 'interdit aux services de renseignement et de sécurité d'exploiter les données recueillies dans les conditions qui ne respectent pas les conditions légales'*. Le Comité a prononcé une seule interdiction de ce genre en 2020 (*infra*).

Enfin, le Comité s'est vu attribuer des modalités de contrôle particulières dans le cadre de la possibilité pour les services de renseignement d'avoir accès à des informations provenant d'images enregistrées par des caméras utilisées par les services de police (article 16/4 L.R&S): un contrôle *a priori* [21] et un contrôle *a posteriori*.[22]

---

20 COMITÉ PERMANENT R, *Rapport d'activités 2017*, 25 note de bas de page 41.

21 '*Les critères d'évaluation visés à l'alinéa 1er, 2°, sont préalablement présentés au Comité permanent R*.'

22 *'La décision du dirigeant du service ou de son délégué et sa motivation sont transmises au Comité permanent R dans les meilleurs délais. La décision peut porter sur un ensemble de données relatives à une enquête de renseignement spécifique. Dans ce cas, une liste des accès ponctuels est communiquée une fois par mois au Comité permanent R. Le Comité permanent R interdit aux services de renseignement et de sécurité d'exploiter les données recueillies dans les conditions qui ne respectent pas les conditions légales'* et *'Chaque liste avec laquelle la corrélation visée à l'alinéa 1er, 1°, est réalisée, est communiquée dans les meilleurs délais au Comité permanent R. Le Comité permanent R interdit aux services de renseignement et de sécurité d'exploiter les données recueillies dans les circonstances qui ne respectent pas les conditions légales*.'

II.2.1.2. Les décisions correctives

L'essentiel des décisions correctives prises par le Comité permanent R dans le cadre de son contrôle de l'utilisation des méthodes ordinaires précitées figurent ci-dessous.

En ce qui concerne la VSSE, deux cas ont donné lieu à une décision de demander un complément d'information, et aucune interdiction d'exploitation n'a été prononcée. Concernant le SGRS, par contre, quatre décisions ont été prises en 2020 dans ce cadre : dans trois cas, un complément d'information a été demandé et une décision d'interdiction d'exploitation a été prononcée. À ce propos, le Comité permanent R fait remarquer que l'article 16/3 le mentionne effectivement, mais qu'interdire l'exploitation sans ordonner une destruction a peu de sens. Une ordonnance de destruction est cependant toujours possible sur la base de la Loi relative à la protection des données. Il semble dès lors indiqué de combiner l'article 16 L.R&S et l'article 51/3 L. Contrôle.

II.2.2. CONTRÔLE DES MÉTHODES PARTICULIÈRES

II.2.2.1. Les chiffres

Cette section reprend les activités du Comité permanent R relatives aux méthodes de renseignement spécifiques et exceptionnelles. L'attention se focalise ici sur les décisions juridictionnelles prises en la matière, et non sur les données opérationnelles. Il convient toutefois de souligner au préalable que le Comité soumet *toutes* les autorisations de mise en œuvre de méthodes particulières à une enquête *prima facie*, et ce en vue de décider d'une éventuelle saisine. Par ailleurs, un membre du Service d'Enquêtes participe à une réunion de quinzaine, au cours de laquelle la VSSE informe la Commission BIM sur l'exécution des méthodes exceptionnelles. Un rapport en est fait à l'intention du Comité, ce qui lui permet d'avoir une meilleure vue sur ces méthodes.[23]

L'article 43/4 L.R&S stipule que le Comité permanent R peut être saisi de cinq manières :

1. D'initiative ;
2. À la demande de l'Autorité de protection des données (APD);
3. Par le dépôt d'une plainte d'un citoyen ;
4. De plein droit, chaque fois que la Commission BIM a suspendu une méthode spécifique ou exceptionnelle pour cause d'illégalité et a interdit l'exploitation des données ;
5. De plein droit, quand le ministre compétent a donné son autorisation sur base de l'article 18/10, § 3 L.R&S.

---

[23] En 2017, le Comité a recommandé au SGRS d'organiser lui aussi de telles réunions de quinzaine. Il s'agit en effet d'une obligation légale (art. 18/10 § 1er, alinéa 3, L.R&S et art. 9 A.R. du 12 octobre 2010). Depuis fin janvier 2018, en raison du nombre restreint de méthodes particulières de renseignement mises en œuvre, une réunion est organisée sur une base mensuelle et, en principe, un rapport est établi sur une base bimensuelle.

Par ailleurs, le Comité peut aussi être saisi en sa qualité d''auteur d'avis préjudiciels' (articles 131*bis*, 189*quater* et 279*bis* CIC). Le cas échéant, le Comité rend un avis sur la légalité des méthodes spécifiques ou exceptionnelles ayant fourni des renseignements qui sont utilisés dans le cadre d'une affaire pénale. Les demandes d'avis sont introduites par les juridictions d'instruction ou par les juridictions de fond. Le Comité n'intervient pas alors *stricto sensu* comme un organe juridictionnel.

TYPE DE SAISINE	2013	2014	2015	2016	2017	2018	2019	2020
1. D'initiative	16	12	16	3	1	1	4	2
2. Commission Vie Privée/ Autorité de protection des données	0	0	0	0	0	0	0	0
3. Plainte	0	0	0	1	0	0	0	0
4. Interdiction d'exploitation par la Commission BIM[24]	5	5	11	19	15	10	12	9
5. Autorisation du ministre	2	1	0	0	0	0	0	0
6. Auteur d'avis préjudiciel	0	0	0	0	0	0	0	0
TOTAL	**23**	**18**	**27**	**23**	**16**	**11**	**16**	**11**

Le nombre de décisions prises par le Comité a continué à diminuer. En outre, toutes les saisines, à deux exceptions près, résultent d'une suspension décidée par la Commission BIM.

Une fois saisi, le Comité peut prendre plusieurs types de décisions et de décisions intermédiaires.

1. Constater la nullité de la plainte pour cause de vice de forme ou absence d'un intérêt personnel et légitime (art. 43/4, alinéa 1er, L.R&S) ;
2. Ne pas donner suite à une plainte qui est manifestement non fondée (art. 43/4, alinéa 1er, L.R&S) ;
3. Suspendre la méthode contestée dans l'attente d'une décision définitive (art. 43/4, dernier alinéa, L.R&S) ;
4. Demander des informations complémentaires à la Commission BIM (43/5 § 1er, alinéa 1er à 3, L.R&S) ;
5. Demander des informations complémentaires au service de renseignement concerné (43/5 § 1er, alinéa 3, L.R&S) ;
6. Ordonner une mission d'enquête pour le service d'Enquêtes R (art. 43/5 § 2 L.R&S). Dans cette rubrique, il est fait référence à la fois aux multiples informations complémentaires recueillies de manière plutôt informelle par le Service d'Enquêtes R avant la saisine proprement dite et aux informations recueillies par le Comité après la saisine ;
7. Procéder à l'audition des membres de la Commission BIM (art. 43/5 § 4, alinéa 1er, L.R&S) ;
8. Procéder à l'audition du dirigeant du service de renseignement ou des membres du service de renseignement concerné (art. 43/5 § 4, alinéa 1er, L.R&S) ;
9. Statuer sur les secrets relatifs à une information ou à une instruction judiciaire en cours dont les membres des services de renseignement sont dépositaires, après concertation avec le magistrat compétent (art. 43/5 § 4, alinéa 2, L.R&S) ;

[24] Elles découlent p.ex de problèmes d'enregistrement ou d'enlèvements d'appareillages.

10. Pour le président du Comité permanent R, statuer, après avoir entendu le dirigeant du service, si le membre du service de renseignement estime devoir garder le secret dont il est dépositaire parce que sa divulgation est de nature à porter préjudice à la protection des sources, à la protection de la vie privée de tiers ou à l'accomplissement des missions du service de renseignement (art. 43/5 § 4, alinéa 3, L.R&S) ;
11. Mettre fin à la méthode concernée si celle-ci est toujours en cours ou si elle a été suspendue par la Commission BIM, et interdire l'exploitation des données recueillies grâce à cette méthode et leur destruction (art. 43/6 § 1er, alinéa 1er, L.R&S) ;
12. Mettre fin partiellement à une méthode autorisée. Il est question ici, par exemple, d'une situation où une méthode est limitée dans le temps, pas d'une situation où une seule autorisation d'un dirigeant du service autorise plusieurs méthodes et où le Comité ne met fin qu'à une seule d'entre elles ;
13. Lever totalement ou partiellement la suspension et l'interdiction qui ont été décidées par la Commission BIM (art. 43/6 § 1er, alinéa 1er, L.R&S). Ceci implique que la méthode autorisée par le dirigeant du service soit (partiellement) considérée comme légale, proportionnelle et subsidiaire par le Comité ;
14. Constater l'incompétence du Comité permanent R ;
15. Déclarer le caractère infondé de l'affaire pendante et permettre la poursuite de la méthode ;
16. Délivrer un 'avis préjudiciel' (art. 131*bis*, 189*quater* et 279*bis* CIC).

NATURE DE LA DÉCISION	2014	2015	2016	2017	2018	2019	2020
Décisions préalables à la saisine							
1. Plainte frappée de nullité	0	0	0	0	0	0	0
2. Plainte manifestement non fondée	0	0	0	0	0	0	0
Décisions intermédiaires							
3. Suspension de la méthode	3	2	1	0	0	0	1
4. Information complémentaire de la Commission BIM	0	0	0	0	0	0	0
5. Information complémentaire du service de renseignement	1	1	4	0	0	0	1
6. Mission d'enquête confiée au Service d'Enquêtes R[25]	54	48	60	35	52	52	24
7. Audition membres de la Commission BIM	0	2	0	0	0	0	0
8.Audition membres des services de renseignement	0	2	0	0	0	1	1
9. Décision relative au secret de l'instruction	0	0	0	0	0	0	0
10. Informations sensibles lors de l'audition	0	0	0	0	0	0	0
Décisions finales							
11. Cessation de la méthode	3	3	6	9	4	11	10
12. Cessation partielle de la méthode	10	13	4	6	6	4	0
13. Levée (partielle) de l'interdiction de la Commission BIM	0	4	11	0	0	0	0

[25] Le Comité demande au Service d'Enquêtes d'effectuer des recherches complémentaires et/ou de contacter le service concerné ou la Commission-BIM.

14. Non compétent	0	0	0	0	0	0	0
15. Autorisation légale/Non- cessation de la méthode/Non-fondement51	4	6	2	1	1	0	0
Avis préjudiciels							
16. Avis préjudiciel	0	0	0	0	0	0	

II.2.2.2. La jurisprudence

La substance des décisions finales prises en 2020 par le Comité permanent R dans le cadre de son rôle juridictionnel est reprise ci-après.[26] Les synthèses sont expurgées des données opérationnelles. Seuls sont mentionnés les éléments qui présentent un intérêt d'un point de vue juridique.

Les décisions ont été regroupées en trois rubriques :

- Les exigences légales (de forme) préalables à la mise en œuvre d'une méthode ;
- La légalité d'une méthode concernant les techniques employées, des données recueillies, la durée de la mesure et la nature de la menace ;
- La légalité de l'exécution d'une méthode légale.

Les exigences légales (de forme) préalables à la mise en œuvre d'une méthode

QUESTION PRÉJUDICIELLE POSÉE À LA COUR CONSTITUTIONNELLE

En 2020, pour la première fois depuis l'entrée en vigueur de la Loi MRD du 4 février 2010, le Comité permanent R a posé une question préjudicielle à la Cour constitutionnelle concernant la législation MRD (dossier 2020/9606).[27] Cette démarche faisait suite à la décision prise par un service de renseignement d'employer des méthodes spécifiques visées à l'article 18/8, § 1er, 1° et 2° L.R&S à l'égard d'un médecin. L'autorisation du dirigeant du service concerné portait plus particulièrement, sur le repérage des données de trafic de moyens de communication électronique à partir desquels ou vers lesquels des communications électroniques sont adressées ou ont été adressées et, d'autre part, sur la localisation de l'origine ou de la destination de communications électroniques. Cette méthode devait viser le numéro de téléphone utilisé par le médecin en question, et ce pour une période de quatre mois précédant la décision du dirigeant du service ainsi que pendant deux mois à compter de la notification de la décision à la Commission BIM. Une méthode ordinaire a permis de découvrir que le numéro de téléphone visé était enregistré en Belgique au seul nom du médecin. Bien que le service de renseignement n'ait pas contesté la qualité de médecin de l'intéressé, le service de renseignement a suivi la procédure d'autorisation normale pour les méthodes spécifiques. Le dirigeant du service a donc pris une 'décision' et l'a ensuite notifiée

[26] Dans certains dossiers, le Comité a été saisi en 2019, mais n'a rendu sa décision finale qu'en 2020.

[27] La Cour constitutionnelle s'était déjà prononcée sur cette législation dans deux arrêts d'annulation (n° 145/2011 et n° 41/2019).

à la Commission BIM (en l'occurrence le même jour). Dès le lendemain, la Commission a ordonné la suspension de la méthode concernée en raison de son caractère illégal.

Selon la Commission, la procédure ordinaire pour les méthodes spécifiques a été utilisée à tort. Compte tenu de la qualité de la personne visée, à savoir celle de médecin, la Commission a estimé qu'il convenait d'appliquer la procédure prévue à l'article 18/3, § 5 L.R&S, à savoir *'(l)es méthodes spécifiques ne peuvent être mise en œuvre à l'égard d'un avocat, d'un médecin ou d'un journaliste, ou de moyens de communication que ceux-ci utilisent à des fins professionnelles qu'à la condition que le service de renseignement et de sécurité dispose au préalable d'indices sérieux attestant que l'avocat, le médecin ou le journaliste participe ou a participé personnellement et activement à la naissance ou au développement de la menace potentielle et après que la commission a rendu, conformément à l'article 18/10, un avis conforme sur le projet de décision du dirigeant du service'*. Cette procédure particulière implique que si un service de renseignement souhaite utiliser une méthode spécifique à l'égard de certaines catégories professionnelles protégées, la procédure des méthodes exceptionnelles doit être suivie, et que toute méthode est soumise, avant sa mise en œuvre, à un contrôle préalable de la Commission BIM. Selon la Commission, il s'agit également d'une exigence en vue de répondre à la procédure visée à l'article 18/2, § 3 L.R&S qui prescrit que si une méthode spécifique ou exceptionnelle *'est mise en œuvre à l'égard d'un avocat, d'un médecin ou d'un journaliste, ou de leurs locaux ou de moyens de communication qu'ils utilisent à des fins professionnelles, ou de leur résidence, ou de leur domicile, cette méthode ne peut être exécutée sans que, suivant le cas, le président de l'Ordre des barreaux francophones et germanophone ou le président de l'Orde van Vlaamse balies, le président du Conseil national de l'Ordre des médecins ou le président de l'Association des journalistes professionnels, ou leur suppléant en cas de maladie ou d'empêchement du président, en soit averti au préalable par le président de la commission visée à l'article 3, 6°. Le président de la commission est tenu de fournir les informations nécessaires au président de l'Ordre ou de l'association des journalistes professionnels dont fait partie l'avocat, le médecin ou le journaliste. Le président concerné et son suppléant sont tenus au secret. (…).'* Si une méthode spécifique ou exceptionnelle '*est mise en œuvre à l'égard d'un avocat, d'un médecin ou d'un journaliste, ou de leurs locaux ou de moyens de communication qu'ils utilisent à des fins professionnelles, ou de leur résidence ou de leur domicile, le président de la commission vérifie si les données obtenues grâce à cette méthode, lorsqu'elles sont protégées par le secret professionnel de l'avocat ou du médecin ou par le secret des sources du journaliste, sont directement liées à la menace potentielle. Si aucun lien direct n'est démontré, la Commission interdit aux services de renseignement et de sécurité d'exploiter ces données.'*. Outre la suspension de la méthode concernée, la Commission BIM a imposé une interdiction d'exploitation pour les données déjà recueillies le cas échéant. La Commission a par ailleurs ordonné une conservation spécifique temporaire de ces données.

Conformément à l'article 43/4 L.R&S, le Comité permanent R est saisi de plein droit chaque fois que la Commission BIM a suspendu l'utilisation d'une méthode spécifique ou d'une méthode exceptionnelle pour cause d'illégalité et a interdit l'exploitation des données pour

cause d'illégalité d'une méthode spécifique ou d'une méthode exceptionnelle. Compte tenu de l'importance du régime de protection particulier dont jouissent les catégories professionnelles précitées et en sa qualité d'organe juridictionnel[28] dans le cadre du contrôle des méthodes spécifiques et exceptionnelles mises en œuvre par les services de renseignement, le Comité a décidé de poser une question préjudicielle à la Cour constitutionnelle. Cette question était motivée comme suit : *'Le Comité permanent R relève que le prescrit de l'article 18/2, § 3, alinéas 1 & 2 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité (L.R&S) restreint la protection accordée aux avocats, médecins et journalistes par rapport aux moyens de communication qu'ils utilisent à des fins professionnelles. Il en découlerait du texte actuel que les moyens de communication à des fins non professionnelles ne seraient pas couverts par la protection légale. Le Comité permanent R se pose la question de savoir comment les services de renseignement peuvent-ils, préalablement, s'assurer de la finalité, professionnelle ou non professionnelle, du moyen de communication concerné (téléphone, GSM…). Est-il possible, a priori, de déterminer dans l'historique des appels téléphoniques d'un avocat, médecin ou journaliste, qu'un numéro présente un caractère exclusivement professionnel. Le législateur n'a pas procédé à cette distinction dans la procédure pénale et plus particulièrement dans les articles 90ter à 90decies du Code d'instruction criminelle. Le législateur a déterminé les conditions strictes auxquelles les services de renseignement, sous le contrôle préalable de la commission BIM, peuvent légalement prendre connaissance des communications conformément à l'article 8, § 2 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (CEDH). (…) Le Comité permanent R constate que l'article 90octies du Code d'instruction criminelle en matière d'interception de communications ou télécommunications, pour les mêmes méthodes et pour les mêmes professions protégées, prévoit une protection indépendamment de la finalité (professionnelle ou non professionnelle) de l'usage de moyen de communication. Cette protection est, donc, différente de celle prévue dans la loi du 30 novembre 1998 sans qu'une justification objective n'apparaisse et semble, dès lors contraire aux principes d'égalité de traitement et de non-discrimination et/ou à l'article 8 de la CEDH.'*.

Le Comité permanent R a décidé de poser la question suivante à la Cour constitutionnelle: *'L'article 18/2 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité viole-t-il les articles 10 et 11 de la Constitution, lus seuls ou conjointement avec l'article 22 de la Constitution et/ou combinés ou non avec l'article 8 de la Convention européenne des droits de l'homme et des libertés fondamentales, signée à Rome le 4 novembre 1950 et approuvée par la loi du 13 mai 1955, en tant qu'il ne prévoit pas en faveur de l'avocat, du médecin ou du journaliste de protection particulière pour les moyens de communication qu'ils utilisent à des fins autre que professionnelles ?*'.

NOTIFICATION TARDIVE DE LA COMMISSION BIM

[28] Cour constitutionnelle, 22 septembre 2011, n° 145/2011, cons. B.38.1

Conformément à l'article 18/3, § 1er, alinéa 2 L.R&S, une méthode spécifique ne peut être mise en œuvre qu'après une décision écrite et motivée du dirigeant du service et après la notification de cette décision à la Commission BIM. Dans le dossier 2020/10.218, le dirigeant du service concerné avait autorisé le recours à un opérateur de télécommunication en vue d'obtenir des données de trafic de moyens de communication électronique à partir desquels ou vers lesquels des communications électroniques sont adressées ou ont été adressées. Cependant, cette décision n'a été notifiée à la Commission BIM qu'un bon mois plus tard. Les données que le service de renseignement a obtenues de l'opérateur de télécommunication pour cette notification avaient donc été obtenues illégalement. Elles devaient par conséquent être détruites par le Comité.

Dans le dossier 2019/8968, un service de renseignement souhaitait prolonger une observation en cours (méthode spécifique). Conformément à l'article 18/3, § 4 L.R&S, l'utilisation de la méthode spécifique ne peut être prolongée (ou renouvelée) que moyennant une nouvelle décision du dirigeant du service et après notification à la Commission BIM. La première méthode spécifique courait du 25 du mois X au 24 du mois Y inclus. Mais ce n'est que le 27 du mois Y que la décision du dirigeant du service de prolonger l'observation a été notifiée à la Commission BIM. À l'instar de l'interdiction d'exploitation prononcée par la Commission BIM, le Comité a décidé que les données recueillies pendant la période non couverte ne pouvaient pas être exploitées et qu'elles devraient être détruites.

Dans le dossier 2020/9595 également, un service de renseignement souhaitait prolonger une observation en cours (méthode spécifique). La première méthode courait jusqu'au 19 du mois X inclus. L'observation en cours devait par conséquent prendre fin à cette date, mais pour des raisons techniques, le recueil d'informations s'est finalement prolongé jusqu'au 26 du mois X inclus. Le dirigeant du service a autorisé la prolongation jusqu'au 26 du mois X, décision qui a été notifiée le 27 à la Commission BIM. Entre le 19 et le 27, les données n'ont donc pas été recueillies légalement. De plus, étant donné que la première observation a pris fin le 19 et que la décision de prolongation n'a été prise par le dirigeant du service que le 26, il ne s'agissait pas *de iure* d'une prolongation de la méthode mais d'un renouvellement. Bien que l'article 18/3, § 4 L.R&S n'établisse pas de distinction entre une prolongation et un renouvellement en ce qui concerne les conditions d'application (en l'occurrence la décision du dirigeant du service et la notification à la Commission BIM), un service de renseignement qui gère la méthode en question doit se montrer plus attentif en cas de prolongation. Sinon, le risque existe qu'il y ait des périodes pendant lesquelles une méthode spécifique n'est pas couverte par une décision notifiée. Dans ce cas, des données sont recueillies en toute illégalité.

MOTIVATION INSUFFISANTE

Dans le cadre d'une méthode spécifique, il était question d'une absence de motivation solide de la décision prise par le dirigeant du service (dossier 2019/8768). Le service de renseignement souhaitait obtenir des données de communications téléphoniques d'une

personne déterminée pour une période de douze mois précédant la date de la décision du dirigeant du service. Le Comité a cependant jugé que la motivation figurant dans la décision MRD ne permettait pas *'te beslissen of de in toepassing gebrachte BIM voldoet aan de door de wet gestelde vereisten, inzake bevoegdheid van de dienst en proportionaliteit van de methode'*.[29] Comme mentionné dans le rapport d'activités 2019, le Comité s'est saisi et a posé une série de questions complémentaires au service de renseignement concerné.[30] Suite à un entretien avec le service de renseignement et une note additionnelle de ce dernier reprenant des informations complémentaires, le Comité a décidé, en 2020, de procéder au retrait de sa saisine, et donc que le service de renseignement était compétent en la matière et que la méthode était proportionnelle.

Dans le dossier 2020/9805, il était aussi question d'une absence de motivation solide. Dans le cas d'espèce, un service de renseignement voulait capturer les enregistrements vidéo et audio d'une conversation qui s'était déroulée dans un lieu non accessible au public et soustrait à la vue (cf. article 18/11, §§ 1er et 2 et article 18/17, §§ 1er et 2 L.R&S). Le Comité n'a cependant pas pu déduire du dossier administratif, principalement constitué de l'autorisation du dirigeant du service et de l'avis conforme de la Commission BIM, pourquoi le service de renseignement a voulu appliquer un tel procédé, ni la finalité exacte de l'opération. Dans ce dossier également, le Comité s'est saisi d'office et a demandé un complément d'information au service de renseignement. Après avoir reçu une note du service de renseignement qui *'op omstandige wijze de werkwijze en de finaliteit van de kwestieuze BIM uiteenzette'*[31] le Comité a décidé que la méthode exceptionnelle était légale.

La légalité d'une méthode concernant les techniques employées, des données recueillies, la durée de la mesure et la nature de la menace

OBJET IMPRÉCIS DE LA MÉTHODE

Dans les dossiers 2020/10.023 et 2020/10.180, il est apparu que le service de renseignement avait mentionné par erreur dans son autorisation un numéro de téléphone qui n'était pas visé par la méthode spécifique en question (en l'occurrence la demande de données de trafic de moyens de communication électronique visés à l'article 18/8, § 1er, 1° L.R&S). La réquisition adressée à l'opérateur de télécommunication mentionnait également ce numéro d'appel erroné. Le service l'a lui-même constaté dans les deux dossiers, mais seulement après l'obtention des données réclamées. Le service de renseignement a systématiquement pris l'initiative de placer les données reçues en quarantaine électronique et a informé la Commission BIM de son erreur. La Commission a interdit l'exploitation des données recueillies illégalement, a averti le Comité permanent R, qui a alors ordonné la destruction

29 *'de décider si la MRD mise en œuvre répond aux exigences légales en termes de compétence du service et de proportionnalité de la méthode.'* (traduction libre)

30 Voir à ce propos : COMITÉ PERMANENT R, *Rapport d'activités 2019*, 56-57.

31 *'a expliqué en détail le procédé et la finalité de la MRD litigieuse.'* (traduction libre)

des données obtenues illégalement.

La légalité de l'exécution d'une méthode légale

MOYENS TECHNIQUES

La Loi organique des services de renseignement décrit un moyen technique comme étant *'une configuration de composants qui détecte des signaux, les transmet, active leur enregistrement et enregistre les signaux'* (art. 3, 14° L.R&S). Un appareil photo et, seulement dans des cas très limités, une caméra mobile[32] ne sont pas considérés comme un moyen technique. Différentes MRD peuvent être mises en œuvre à l'aide de moyens techniques. Dans le dossier 2019/8987, il a été fait usage d'une caméra munie d'un microphone, et le dirigeant du service a donné son autorisation après l'avis conforme de la Commission BIM (en l'occurrence pour la méthode prévue à l'article 18/11 L.R&S – observation comme méthode exceptionnelle – en combinaison avec la méthode prévue à l'article 18/17 L.R&S – écoute téléphonique). L'autorisation courait jusqu'au 3 du mois, mais l'appareil a continué à faire des enregistrements vidéo et audio après cette date, et ce *'om technische redenen, omdat de camera met microfoon niet van op afstand kon bediend worden.'*[33] Ainsi, *'(bleef) de geplaatste camera (…) beelden maken en de microfoon verder geluid (opnemen)'*[34]même s'il n'y avait plus d'autorisation. Le Comité a suivi l'interdiction d'exploitation prononcée par la Commission BIM pour les données recueillies après cette date et a ordonné leur destruction.

Dans le dossier 2020/9595 mentionné précédemment, il n'a pas été mis fin à une observation (méthode spécifique) pour des raisons techniques et le Comité, après intervention de la Commission BIM, a ordonné la destruction des données recueillies illégalement.

DIFFÉRENCE ENTRE L'AUTORISATION DU DIRIGEANT DU SERVICE ET LA RÉQUISITION

Dans trois décisions, l'autorisation du dirigeant du service en vue de mettre en œuvre une méthode spécifique ou exceptionnelle s'avérait parfaitement légale, mais un problème s'est posé au niveau de l'exécution, en ce sens que la réclamation des données ne correspondait pas au mandat initial. Soit le délai de mise sur écoute figurant dans la réquisition ne correspondait avec celui qui était repris dans l'autorisation (dossier 2020/9204), soit un

---

32 Est plus particulièrement exclu *'un appareil mobile utilisé pour la prise d'images animées lorsque la prise de photographies ne permet pas de garantir la discrétion et la sécurité des agents et à la condition que cette utilisation ait été préalablement autorisée par le dirigeant du service ou son délégué'*. Dans un tel cas, *'seules les images fixes jugées pertinentes sont conservées. Les autres images sont détruites dans le mois qui suit le jour de l'enregistrement'* (art. 3, 14°, b L.R&S).

33 *'pour des raisons techniques, car la caméra munie d'un microphone ne pouvait pas être contrôlée à distance'.'*(traduction libre)

34 *'la caméra qui était installée a continué à produire des images et le microphone, à enregistrer des sons'*. (traduction libre)

numéro de téléphone erroné a été communiqué au fournisseur de télécommunication (dossier 2019/8964), ou encore *'(werd) per vergissing aan de uitvoerende telecommunicatiedienst niet alleen een eenmalige intrusie (…) gevraagd'*[35], plus précisément un *'eenmalige toegang (…) tot het mailverkeer'* [36] du target (cf. art. 18/16 L.R&S), *'maar (…) werd (ook) gevraagd om een live acces te voorzien'*[37] (dossier 2020/9829). Un élément qui mérite d'être mentionné dans ce dernier cas est le fait que le service de renseignement a lui-même constaté cette erreur et a ensuite pris l'initiative, conformément à l'article 18/10, § 1er, alinéa 4 L.R&S de mettre fin au *'live access'*. Le service de renseignement a décidé de conserver à part les données recueillies illégalement. La Commission BIM a dès lors prononcé une interdiction d'exploitation et a également prévu une conservation spécifique temporaire. Enfin, le Comité a confirmé l'interdiction d'exploitation prononcée par la Commission BIM et a ordonné la destruction des données obtenues via le *'live access'*.

DONNÉES ERRONNÉES FOURNIES PAR L'OPÉRATEUR OU LE FOURNISSEUR DE TÉLÉCOMMUNICATION

Dans trois cas distincts, un service de renseignement avait réquisitionné légalement l'opérateur de réseau concerné, mais la transmission des données réclamées posait un problème dans la mesure où les données transmises par l'opérateur n'avaient aucun rapport avec les données réclamées. Dans les dossiers 2020/9167 et 2020/9225, il s'agissait chaque fois d''*een telefonie-onderzoek en een afluistermaatregel'*[38], portant respectivement sur trois et deux numéros de téléphone. Dans le dossier 2019/8934, il était uniquement question d'une réquisition dans le cadre du repérage de données de trafic et de localisation de moyens de communication électronique. Dans les trois cas, *'(werden) de betreffende data op wederrechtelijke wijze (…) meegedeeld aan'*[39] service de renseignement concerné. Cela s'est donc produit *'buiten de wil van'*[40] service de renseignement *'om'*[41]. Dans tous les cas, la Commission BIM a prononcé une interdiction d'exploitation, suivie par une ordonnance de destruction du Comité.

II.3. CONCLUSIONS

Le Comité permanent R formule les conclusions générales suivantes :

---

35 *'Ce n'est pas seulement une intrusion ponctuelle qui a été demandée à tort au service de télécommunications concerné par la réquisition'* (traduction libre)

36 *'un accès ponctuel (…) aux échange d'e-mails'* (traduction libre)

37 *'mais il a aussi été demandé de prévoir un live access.' (traduction libre)*

38 *'une enquête de téléphonie et d'une opération de mise sur écoute'* (traduction libre)

39 *'les données concernées ont été communiquées illégalement au'* (traduction libre)

40 *'indépendamment de la volonté du'* (traduction libre)

41 *'pour'* (traduction libre)

- Entre le 1er janvier 2020 et le 31 décembre 2020, 2337 autorisations ont été émises par les deux services de renseignement confondus pour l'utilisation de méthodes particulières de renseignement : 2140 par la VSSE (1629 spécifiques et 511 exceptionnelles) et 197 par le SGRS (146 spécifiques et 51 exceptionnelles). Après une augmentation constante du nombre de MRD mises en œuvre ces dernières années et une stagnation observée l'année dernière, on remarque pour la première fois une légère diminution. Selon les responsables MRD de la VSSE et du SGRS, la pandémie de COVID n'a eu aucun impact sur le nombre de méthodes particulières de renseignement mises en œuvre.
- La VSSE continue de se tailler la part du lion, avec 91,5 % des méthodes mises en œuvre. En d'autres termes, moins d'1 méthode sur 10 est mise en œuvre par le SGRS.
- Une ventilation de ces chiffres permet de constater que l'augmentation du nombre de méthodes spécifiques par le SGRS se poursuit, passant de 138 à 146. Le nombre de méthodes exceptionnelles mises en œuvre connaît toutefois une forte diminution d'environ un tiers, passant de 76 à 51. À la VSSE, on observe la tendance inverse, c'est-à-dire une diminution remarquable de l'utilisation des méthodes spécifiques (de 1781 en 2019 à 1629 en 2020) et une nouvelle hausse sensible de l'utilisation des méthodes exceptionnelles (de 449 en 2019 à 511 en 2020, soit une hausse d'environ 14 %).
- En ce qui concerne les méthodes ordinaires qui consistent à adresser une réquisition à des opérateurs afin d'identifier certains moyens de communication, on note de nouveau une diminution d'environ 9 %, que soit pour la VSSE ou le SGRS.
- On peut encore noter que les MRD mises en œuvre dans le cadre des menaces 'terrorisme' et 'extrémisme' ont connu une hausse sensible, au détriment de la menace 'ingérence', qui a diminué de moitié.
- Dans le contexte de la mise en œuvre des méthodes particulières de renseignement, le SGRS s'est surtout concentré sur les menaces 'terrorisme' et 'extrémisme', au détriment de la menace 'ingérence', qui a diminué de moitié. La VSSE a, quant à elle, focalisé son attention sur le 'terrorisme', suivi par la menace 'espionnage'.
- Le Comité a été saisi dans 11 dossiers, à savoir 2 saisines d'initiative et 9 saisines de plein droit, après la suspension décidée par la Commission BIM pour illégalité (art. 43/4 L.R&S). Les illégalités concernaient notamment une motivation insuffisante, une notification tardive de la Commission BIM, ou encore un objet imprécis.
- En 2020, pour la première fois depuis l'entrée en vigueur de la Loi MRD du 4 février 2010, le Comité permanent R a posé une question préjudicielle à la Cour constitutionnelle concernant la législation MRD. Cette affaire est pendante.